MISURE MINIME DI SICUREZZA

Le misure minime di sicurezza sono contenute negli articoli dal 33 al 36 del Codice Privacy e definite tecnicamente nell'Allegato B dello stesso. Pur essendo, per definizione, un disciplinare tecnico, il linguaggio è spesso di difficile interpretazione. Per questa ragione vi invitiamo a leggere le interpretazioni da noi suggerite ad ogni articolo: se le giudicate non sufficientemente chiare inviate una e-mail a info@poloconsulting.net
Con il Provvedimento del 27 novembre 2008 (vedi la sezione Provvedimenti normativi alla pagina del **GARANTE**), pubblicato sulla G.U. n. 287 del 9 dicembre 2008, il Garante ha semplificato le norme relative alle misure minime di sicurezza per le piccole e medie imprese, gli studi professionali, gli artigiani e le imprese che non trattano dati sensibili o giudiziari. In particolare, il Codice Privacy ora suddivide i gestori dei trattamenti in:

A. **aziende che trattano i dati personali anche per fini diversi da quelli amministrativi e contabili, o che comunque non rientrano tra quelle delle categorie B e C**
   appartengono a questa categoria, a puro titolo esemplificativo, tutte le aziende ed i liberi professionisti dei settori sanitario, giuridico, di selezione del personale per conto terzi, di profilazione per sondaggi d'opinione o ricerche di mercato, ecc.;

B. **aziende che trattano i dati personali esclusivamente per fini amministrativi e contabili, in particolare liberi professionisti, artigiani e piccole e medie imprese**
   appartengono a questa categoria tutte le aziende, i liberi professionisti ed i lavoratori autonomi che trattano dati personali per fini amministrativi e contabili;
   l'Ufficio del Garante ha precisato che **nei fini amministrativi e contabili sono inclusi i trattamenti di dati sensibili conseguenti ad obblighi di legge**, purché detti trattamenti non siano l'oggetto primario dell'attività sociale. Ciò vuol dire che, ad esempio, i commercialisti, i consulenti del lavoro, i concessionari, i mediatori del credito, ecc., appartengono a questa categoria;

C. **aziende che trattano dati personali non sensibili o dati sensibili dei loro dipendenti o collaboratori, relativi allo stato di salute, senza indicazione della diagnosi, o all'adesione ai sindacati**
   appartengono a questa categoria tutte le aziende, pubbliche e private, i liberi professionisti ed i lavoratori autonomi che trattano esclusivamente i dati sensibili dei loro dipendenti per osservare obblighi di legge, cioè quelli relativi alle dichiarazioni di malattia o all'adesione al sindacato.

I soggetti di cui al comma **A** devono adempiere integralmente a quanto prescritto nel disciplinare tecnico di cui all'Allegato B del Codice Privacy.
In particolare, essi sono tenuti a redigere ed aggiornare il Documento Programmatico sulla Sicurezza.

I soggetti di cui al comma **B** devono adempiere a quanto prescritto nel disciplinare tecnico di cui all'Allegato B del Codice Privacy, interpretando le norme secondo quanto prescritto nel Provvedimento del Garante del 27 novembre 2008.
In particolare, essi devono redigere ed aggiornare il Documento Programmatico sulla Sicurezza semplificato o Documento Semplificato sulla Sicurezza e, se non esistono variazioni, compilare la Dichiarazione di estensione di validità.
Vi precisiamo che:

- in base all'art. 2083 del Codice Civile, "*sono piccoli imprenditori i coltivatori diretti del fondo, gli artigiani, i piccoli commercianti e coloro che esercitano un'attività professionale organizzata prevalentemente con il lavoro proprio e dei componenti della famiglia*";
- in base all'art. 2 del D.M. del 18 aprile 2005, "*La categoria delle microimprese, delle piccole imprese e delle medie imprese (complessivamente definita PMI) è costituita da*

imprese che hanno meno di 250 occupati e hanno un fatturato annuo non superiore a 50 milioni di euro, oppure un totale di bilancio annuo non superiore a 43 milioni di euro.
Nell'ambito della categoria delle PMI, si definisce piccola impresa l'impresa che ha meno di 50 occupati, e ha un fatturato annuo oppure un totale di bilancio annuo non superiore a 10 milioni di euro.
Nell'ambito della categoria delle PMI, si definisce microimpresa l'impresa che ha meno di 10 occupati, e ha un fatturato annuo oppure un totale di bilancio annuo non superiore a 2 milioni di euro."

I soggetti di cui al comma **C** devono adempiere a quanto prescritto nel disciplinare tecnico di cui all'Allegato B del Codice Privacy, interpretando le norme secondo quanto prescritto dal Provvedimento del Garante del 27 novembre 2008, eccetto la redazione del Documento Semplificato sulla Sicurezza (punto 2.5), che può essere sostituita da una Dichiarazione sostitutiva dell'atto di notorietà ai sensi dell'art. 47 del D.P.R. 445/2000.

In calce a questo file troverete la tabella riassuntiva delle misure minime di sicurezza per ognuna delle tipologie di azienda sopraccitate.

A **Aziende che trattano i dati personali anche per fini diversi da quelli amministrativi e contabili, e che comunque non rientrano tra quelle comprese nelle categorie B e C**

Queste aziende sono tenute alla totale osservanza di quanto disposto dal:

Allegato B

DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA
(Artt. da 33 a 36 del codice)

Trattamenti con strumenti elettronici

Modalità tecniche da adottare a cura del titolare, del responsabile ove designato e dell'incaricato, in caso di trattamento con strumenti elettronici:

Per strumenti elettronici si intendono i computer, i server, le carte di accesso, i sistemi biometrici di riconoscimento, le videocamere, ecc. Nel seguito citeremo genericamente i soli computer, salvo quando l'articolo si riferisce specificatamente ad un altro strumento elettronico.

Sistema di autenticazione informatica

1. *Il trattamento di dati personali con strumenti elettronici è consentito agli incaricati dotati di credenziali di autenticazione che consentano il superamento di una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti.*

L'accesso a qualunque computer deve avvenire esclusivamente tramite "credenziali di autenticazione", introdotte da Incaricati abilitati dal Titolare.

2. *Le credenziali di autenticazione consistono in un codice per l'identificazione dell'incaricato associato a una parola chiave riservata conosciuta solamente dal medesimo oppure in un dispositivo di autenticazione in possesso e uso esclusivo dell'incaricato, eventualmente associato a un codice identificativo o a una parola chiave, oppure in una caratteristica biometria dell'incaricato, eventualmente associata a un codice identificativo o a una parola chiave.*

Le credenziali di autenticazione sono costituite da una UserName, assegnata dal Titolare, e da una Password, introdotta dall'Incaricato.
Se l'accesso avviene tramite una carta di accesso ad uso esclusivo dell'Incaricato, le credenziali possono essere contenute nella stessa.
Se l'accesso avviene tramite un dispositivo biometrico di riconoscimento, le credenziali possono essere contenute nel dispositivo stesso.

3. *Ad ogni incaricato sono assegnate o associate individualmente una o più credenziali per l'autenticazione.*

Ad ogni incaricato possono essere fornite una o più Username. Per motivi di sicurezza, ad ogni UserName deve corrispondere una Password diversa.

4. *Con le istruzioni impartite agli incaricati è prescritto di adottare le necessarie cautele per assicurare la segretezza della componente riservata della credenziale e la diligente custodia dei dispositivi in possesso ed uso esclusivo dell'incaricato.*

La UserName è nota solo al Titolare, al Responsabile ed agli Incaricati al trattamento, mentre la Password è personale e segreta. Il Titolare, od un Incaricato alla Custodia delle Password nominato dallo stesso, deve

custodire le Password in un contenitore protetto, senza prenderne visione eccetto nei casi di cui alla successiva regola 10. Inoltre il Titolare deve impartire istruzioni scritte, nella lettera d'incarico e/o nel Mansionario Privacy, sull'utilizzo e la protezione delle credenziali di autenticazione.

5. *La parola chiave, quando è prevista dal sistema di autenticazione, è composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito; essa non contiene riferimenti agevolmente riconducibili all'incaricato ed è modificata da quest'ultimo al primo utilizzo e, successivamente, almeno ogni sei mesi. In caso di trattamento di dati sensibili e di dati giudiziari la parola chiave è modificata almeno ogni tre mesi.*

La Password deve essere lunga almeno otto caratteri, non deve contenere riferimenti all'Incaricato (nome e/o cognome dell'Incaricato, di suoi parenti, amici, animali, ecc.), deve essere modificata al primo utilizzo ed almeno ogni sei mesi (almeno ogni tre mesi se l'Incaricato tratta dati sensibili e/o giudiziari).
Ad ogni cambio Password l'Incaricato dovrà fornire, in busta chiusa, al Titolare od all'Incaricato alla Custodia delle Parole Chiave il testo della stessa.
Per primo utilizzo si intende la prima volta che l'incaricato accede al computer e quando la sua Password è stata utilizzata, in sua assenza, da altri incaricati (vedi regola 10)

6. *Il codice per l'identificazione, laddove utilizzato, non può essere assegnato ad altri incaricati, neppure in tempi diversi.*

La UserName non può essere mai essere assegnata ad un altro Incaricato abilitato o rimosso.

7. *Le credenziali di autenticazione non utilizzate da almeno sei mesi sono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica.*

Le credenziali di autenticazione, escluse quelle per la gestione tecnica, non utilizzate da almeno sei mesi devono essere disattivate.

8. *Le credenziali sono disattivate anche in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali.*

Se l'Incaricato è stato rimosso dall'incarico, per dimissioni, licenziamento, fine contratto o nuove mansioni, le sue credenziali di autenticazione devono essere disattivate.

9. *Sono impartite istruzioni agli incaricati per non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento.*

L'Incaricato, durante le assenze temporanee, deve attivare il dispositivo di blocco del computer (screen saver protetto da password), Al termine della giornata lavorativa deve spegnere il computer, eccetto che lo stesso sia un server. Le istruzioni devono essere scritte.

10. *Quando l'accesso ai dati e agli strumenti elettronici è consentito esclusivamente mediante uso della componente riservata della credenziale per l'autenticazione, sono impartite idonee e preventive disposizioni scritte volte a individuare chiaramente le modalità con le quali il titolare può assicurare la disponibilità di dati o strumenti elettronici in caso di prolungata assenza o impedimento dell'incaricato che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema. In tal caso la custodia delle copie delle credenziali è organizzata garantendo la relativa segretezza e individuando preventivamente per iscritto i soggetti incaricati della loro custodia, i quali devono informare tempestivamente l'incaricato dell'intervento effettuato.*

Se il Titolare o l'Incaricato all'Amministrazione del Sistema, per motivi tecnici od organizzativi improcrastinabili, devono accedere ad un computer di cui non conoscono la Password e l'Incaricato è assente, il Titolare o l'Incaricato alla Custodia delle Parole Chiave possono reperirla dalla busta relativa all'Incaricato. L'Incaricato alla Custodia delle Parole Chiave, od il Titolare, avviseranno al suo rientro l'Incaricato, il quale dovrà inserire una nuova Password. Tutte le operazioni effettuate, compresi le periodiche sostituzioni delle Password, sono registrate a cura dell'Incaricato alla Custodia delle Password.

***11.** Le disposizioni sul sistema di autenticazione di cui ai precedenti punti e quelle sul sistema di autorizzazione non si applicano ai trattamenti dei dati personali destinati alla diffusione.*

Tutte le disposizioni di cui alle regole da 1 a 10 non si applicano se il trattamento riguarda esclusivamente dati personali diffusi, cioè disponibili a tutti. Vi ricordiamo che possono essere diffusi esclusivamente quelli di dominio pubblico o quelli per i quali avete ottenuto il consenso scritto dall'interessato, purché non siano dati sensibili o giudiziari.

Sistema di autorizzazione

***12.** Quando per gli incaricati sono individuati profili di autorizzazione di ambito diverso è utilizzato un sistema di autorizzazione.*

Funzioni specifiche (es. Internet) o particolari base dati (es. Banche) possono essere inibite ad alcuni incaricati. In tal caso l'accesso deve essere effettuato tramite un sistema di autorizzazione, controllato dal sistema operativo.

***13.** I profili di autorizzazione, per ciascun incaricato o per classi omogenee di incaricati, sono individuati e configurati anteriormente all'inizio del trattamento, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento.*

I profili di autorizzazione, cioè la definizione di cosa l'incaricato può fare con funzioni specifiche o su particolari base dati, devono essere definiti prima di iniziare il trattamento.

***14.** Periodicamente, e comunque almeno annualmente, è verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione.*

Almeno annualmente occorre verificare la necessità di ogni profilo di autorizzazione e, se è il caso, modificarlo o cancellarlo.

Altre misure di sicurezza

***15.** Nell'ambito dell'aggiornamento periodico con cadenza almeno annuale dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici, la lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione.*

Almeno annualmente bisogna redigere una lista degli Incaricati, completa del gruppo di lavoro di appartenenza e dei relativi profili di autorizzazione, se esistono.

***16.** I dati personali sono protetti contro il rischio di intrusione e dell'azione di programmi di cui all'art. 615-quinquies del codice penale, mediante l'attivazione di idonei strumenti elettronici da aggiornare con cadenza almeno semestrale.*

I dati personali devono essere protetti contro il rischio di intrusione o di accessi non consentiti da appositi dispositivi software (antivirus) da aggiornare almeno ogni sei mesi.
Vi consigliamo vivamente di aggiornare questi software automaticamente, o almeno settimanalmente, altrimenti non potrete più utilizzare i computer perché saranno infettati da ogni sorta di virus che renderanno inaffidabili e, spesso, illeggibili i vostri dati.

***17.** Gli aggiornamenti periodici dei programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti sono effettuati almeno annualmente. In caso di trattamento di dati sensibili o giudiziari l'aggiornamento è almeno semestrale.*

I dati personali devono essere protetti contro il rischio di intrusione o di accessi non consentiti da aggiornamenti del software di sistema e applicativo almeno annuale. Se il trattamento riguarda dati sensibili o giudiziari, gli aggiornamenti devono avvenire almeno ogni sei mesi.
Vi consigliamo vivamente di aggiornarli automaticamente: spesso contengono correzioni di errori del software originale o modifiche essenziali per la tutela dei vostri dati.

***18.** Sono impartite istruzioni organizzative e tecniche che prevedono il salvataggio dei dati con frequenza almeno settimanale.*

I dati personali devono essere protetti contro il rischio di perdita accidentale da salvataggi totali almeno settimanali. Le istruzioni devono essere scritte.

Documento programmatico sulla sicurezza

Per sapere chi deve, perché, come e quando compilare questo documento, leggete il file **DPSS** alla pagina **ADEMPIMENTI PERIODICI**.

***19.** Entro il 31 marzo di ogni anno, il titolare di un trattamento di dati sensibili o di dati giudiziari redige anche attraverso il responsabile, se designato, un documento programmatico sulla sicurezza contenente idonee informazioni riguardo:*

Il documento deve essere redatto o aggiornato entro il 31 marzo di ogni anno.

***19.1.** l'elenco dei trattamenti di dati personali;*

L'elenco dei trattamenti deve comprendere le finalità e le modalità dello stesso.

***19.2.** la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati;*

L'elenco dei Responsabili e degli Incaricati deve indicare, per ognuno di essi, i rispettivi compiti generali e specifici.

***19.3.** l'analisi dei rischi che incombono sui dati;*

L'analisi dei rischi deve essere effettuata in base a metodologie certificate o, comunque, tecnicamente valide.

***19.4.** le misure da adottare per garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità;*

L'elenco delle misure di sicurezza adottate deve essere preceduto da una descrizione della Sede Operativa, per dare un contesto alle stesse.

***19.5.** la descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento di cui al successivo punto 23;*

La norma si riferisce alla descrizione della procedura di "**Disaster Recovery**" citata al successivo punto 23.

***19.6.** la previsione di interventi formativi degli incaricati del trattamento, per renderli edotti dei rischi che incombono sui dati, delle misure disponibili per prevenire eventi dannosi, dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure minime adottate dal titolare. La formazione è programmata già al momento dell'ingresso in servizio, nonché in occasione di cambiamenti di mansioni, o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali;*

Il documento deve comprendere il piano di formazione aziendale per l'anno in corso. Tutti gli Incaricati devono, almeno una volta, partecipare ad un corso di formazione sulla protezione dei dati personali, tenuto dal Titolare o da personale interno o esterno avente i requisiti richiesti dal Codice Privacy.

***19.7.** la descrizione dei criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti di dati personali affidati, in conformità al codice, all'esterno della struttura del titolare;*

Nella maggior parte dei casi, per ogni trattamento affidato all'esterno (outsourcing), è richiesta una dichiarazione del soggetto esterno che si impegna a trattare i dati secondo quanto disposto dal Codice Privacy.

In tal caso, nel documento occorre identificare i soggetti ed allegare le dichiarazioni.

19.8.*per i dati personali idonei a rivelare lo stato di salute e la vita sessuale di cui al punto 24, l'individuazione dei criteri da adottare per la cifratura o per la separazione di tali dati dagli altri dati personali dell'interessato.*

Coloro che trattano dati sensibili relativi allo stato di salute e la vita sessuale devono adottare un sistema di cifratura per le base dati che li contengono oppure separare tali dati da quelli non sensibili.
Il documento deve riportare le decisioni adottate.

Ulteriori misure in caso di trattamento di dati sensibili o giudiziari

20.*I dati sensibili o giudiziari sono protetti contro l'accesso abusivo, di cui all'art. 615-ter del codice penale, mediante l'utilizzo di idonei strumenti elettronici.*

I dati personali sensibili o giudiziari devono essere protetti contro il rischio di accessi non consentiti da appositi dispositivi software o hardware (firewall, antispyware, ecc.).

21.*Sono impartite istruzioni organizzative e tecniche per la custodia e l'uso dei supporti rimovibili su cui sono memorizzati i dati al fine di evitare accessi non autorizzati e trattamenti non consentiti.*

I supporti removibili (floppy-disk, cdrom, pen-key, ecc.) contenenti dati personali sensibili o giudiziari devono essere archiviati in contenitori protetti. Se trasportati al di fuori della Sede Operativa, i dati in essi contenuti devono essere in formato protetto (file con password di accesso o cifrati). Le istruzioni devono essere scritte.

22.*I supporti rimovibili contenenti dati sensibili o giudiziari se non utilizzati sono distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altri incaricati, non autorizzati al trattamento degli stessi dati, se le informazioni precedentemente in essi contenute non sono intelligibili e tecnicamente in alcun modo ricostruibili.*

I supporti removibili contenenti dati personali sensibili o giudiziari non più utilizzati devono essere fisicamente distrutti o riutilizzati dopo la loro completa formattazione.
Vi informiamo che un utente esperto può ricavare i dati originali anche da un disco formattato: quindi è sempre meglio distruggerli.

23.*Sono adottate idonee misure per garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati e non superiori a sette giorni.*

Se trattate dati sensibili e/o giudiziari dovete prevedere una procedura di ripristino dei dati (**Disaster Recovery**) da attivare in caso di anomalie sui dati e/o sui computer. In proposito leggete il file **Mansionario** alla pagina **ADEMPIMENTI PERIODICI**.
Il ripristino della disponibilità dei dati deve avvenire entro sette giorni.

24.*Gli organismi sanitari e gli esercenti le professioni sanitarie effettuano il trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale contenuti in elenchi, registri o banche di dati con le modalità di cui all'articolo 22, comma 6, del codice, anche al fine di consentire il trattamento disgiunto dei medesimi dati dagli altri dati personali che permettono di identificare direttamente gli interessati. I dati relativi all'identità genetica sono trattati esclusivamente all'interno di locali protetti accessibili ai soli incaricati dei trattamenti ed ai soggetti specificatamente autorizzati ad accedervi; il trasporto dei dati all'esterno dei locali riservati al loro trattamento deve avvenire in contenitori muniti di serratura o dispositivi equipollenti; il trasferimento dei dati in formato elettronico è cifrato.*

Se trattate dati sensibili in ambito sanitario utilizzando elenchi, registri o banche dati, dovete prevedere una procedura di separazione dei dati sensibili da quelli identificativi, cifrandoli o utilizzando codici identificativi, tali da renderli anonimi.
I dati genetici devono essere trattati in locali protetti, accessibili ai soli Incaricati del trattamento. Se trasportati al di fuori dei locali di cui sopra, devono essere posti in contenitori dotati di serratura. Se trasmessi via e-mail devono essere cifrati.

Misure di tutela e garanzia

25.*Il titolare che adotta misure minime di sicurezza avvalendosi di soggetti esterni alla propria struttura, per provvedere alla esecuzione riceve dall'installatore una descrizione scritta dell'intervento effettuato che ne attesta la conformità alle disposizioni del presente disciplinare tecnico.*

Se utilizzate un consulente informatico esterno per installare o manutenere hardware o software, al termine del lavoro, dovrete farvi rilasciare una descrizione scritta dell'intervento effettuato ed una dichiarazione di conformità al presente disciplinare tecnico.
La stessa dichiarazione di conformità deve essere rilasciata da tutti i tecnici che installano o mantengono gli impianti e le apparecchiature relative alla sicurezza della Sede Operativa, come, ad esempio, l'impianto d'allarme o quello antincendio.

26.*Il titolare riferisce, nella relazione accompagnatoria del bilancio d'esercizio, se dovuta, dell'avvenuta redazione o aggiornamento del documento programmatico sulla sicurezza.*

Se siete tenuti ad allegare al Bilancio d'Esercizio la Relazione Accompagnatoria, dovete indicare nella stessa che avete redatto o aggiornato il Documento Programmatico Sulla Sicurezza.
Dovete solo comunicare al professionista incaricato di elaborare il Bilancio che avete redatto o aggiornato il **DPSS**: ci penserà lui!

Trattamenti senza l'ausilio di strumenti elettronici

Modalità tecniche da adottare a cura del titolare, del responsabile, ove designato, e dell'incaricato, in caso di trattamento con strumenti diversi da quelli elettronici:

Per strumenti diversi da quelli elettronici si intendono essenzialmente tutti gli archivi cartacei.

27.*Agli incaricati sono impartite istruzioni scritte finalizzate al controllo ed alla custodia, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti e dei documenti contenenti dati personali. Nell'ambito dell'aggiornamento periodico con cadenza almeno annuale dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati, la lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione.*

Tutti gli incaricati devono ricevere istruzioni scritte circa i trattamenti consentiti e la custodia dei dati affidati. Come per i trattamenti con strumenti elettronici (vedi regola 15), almeno annualmente bisogna redigere una lista degli Incaricati, completa del gruppo di lavoro di appartenenza e dei relativi profili di autorizzazione, se esistono.

28.*Quando gli atti e i documenti contenenti dati personali sensibili o giudiziari sono affidati agli incaricati del trattamento per lo svolgimento dei relativi compiti, i medesimi atti e documenti sono controllati e custoditi dagli incaricati fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate.*

I documenti contenenti dati personali sensibili o giudiziari devono essere "guardati a vista" dall'Incaricato ed archiviati in un contenitore protetto al termine della loro consultazione, o consegnati nelle mani dell'Incaricato alla Custodia della Sede Operativa.

29.*L'accesso agli archivi contenenti dati sensibili o giudiziari è controllato. Le persone ammesse, a qualunque titolo, dopo l'orario di chiusura, sono identificate e registrate. Quando gli archivi non sono dotati di strumenti elettronici per il controllo degli accessi o di incaricati della vigilanza, le persone che vi accedono sono preventivamente autorizzate.*

L'accesso agli archivi contenenti dati sensibili o giudiziari, dopo l'orario di chiusura, deve essere riportato su un apposito Registro di consultazione contenente i dati personali dell'Incaricato e l'orario d'accesso. Tutti gli Incaricati devono essere preventivamente autorizzati e, se previsto, forniti di una carta d'accesso personale.
La tenuta del Registro di consultazione può essere affidata al Titolare o al Responsabile o all'Incaricato alla Custodia della Sede Operativa.

B Aziende che trattano i dati personali esclusivamente per fini amministrativi e contabili, in particolare liberi professionisti, artigiani e piccole e medie imprese

Queste aziende sono tenute alla totale osservanza di quanto disposto dall'**Allegato B** al Codice Privacy con i criteri applicativi esposti nel:

Provvedimento del Garante del 27 novembre 2008

Misure semplificate per applicare le misure minime di sicurezza nel trattamento dei dati personali

1. Soggetti che possono avvalersi della semplificazione

Le seguenti modalità semplificate sono applicabili dai soggetti pubblici o privati che:

a) utilizzano dati personali non sensibili o che trattano come unici dati sensibili riferiti ai propri dipendenti e collaboratori anche a progetto quelli costituiti dallo stato di salute o malattia senza indicazione della relativa diagnosi, ovvero dall'adesione a organizzazioni sindacali o a carattere sindacale;

aziende della categoria **C**

b) trattano dati personali unicamente per correnti finalità amministrative e contabili, in particolare presso liberi professionisti, artigiani e piccole e medie imprese (cfr. art. 2083 Cod. Civ. e D.M. del 18 aprile 2005, recante adeguamento alla disciplina comunitaria dei criteri di individuazione di piccole e medie imprese, pubblicato nella Gazzetta Ufficiale 12 ottobre 2005, n. 238).

aziende della categoria **B**

2. Trattamenti effettuati con strumenti elettronici

I soggetti di cui al paragrafo 1 possono applicare le misure minime di sicurezza prescritte dalla disciplina in materia di trattamenti realizzati con l'ausilio di strumenti elettronici (art. 34 del Codice e regole da 1 a 26 dell'Allegato B) osservando le modalità semplificate di seguito individuate.

L'utilizzo delle misure di sicurezza semplificate è autorizzato solo per le aziende delle categorie **B** e **C**.

2.1. Istruzioni agli incaricati del trattamento (modalità applicative delle regole di cui ai punti 4, 9, 18 e 21 dell'Allegato B)

Le istruzioni in materia di misure minime di sicurezza previste dall'Allegato B) possono essere impartite agli incaricati del trattamento anche oralmente, con indicazioni di semplice e chiara formulazione.

Ovunque sono richieste istruzioni circa il trattamento o l'uso degli strumenti per effettuarli, esse possono essere orali.

2.2. *Sistema di autenticazione informatica (modalità applicative delle regole 1, 2, 3, 5, 6, 7, 8, 10, 11 dell'Allegato B)*

Per l'accesso ai sistemi informatici si può utilizzare un qualsiasi sistema di autenticazione basato su un codice per identificare chi accede ai dati (di seguito, "username"), associato a una parola chiave (di seguito: "password"), in modo che:

a) l'username individui in modo univoco una sola persona, evitando che soggetti diversi utilizzino codici identici;

b) la password sia conosciuta solo dalla persona che accede ai dati.

L'username deve essere disattivato quando l'incaricato non ha più la qualità che rende legittimo l'utilizzo dei dati (ad esempio, in quanto non opera più all'interno dell'organizzazione).

Può essere adottata, quale procedura di autenticazione anche la procedura di login disponibile sul sistema operativo delle postazioni di lavoro connesse a una rete.

In caso di prolungata assenza o impedimento dell'incaricato che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema, se l'accesso ai dati e agli strumenti elettronici è consentito esclusivamente mediante uso della password, il titolare può assicurare la disponibilità di dati o strumenti elettronici con procedure o modalità predefinite. Riguardo a tali modalità, sono fornite preventive istruzioni agli incaricati e gli stessi sono informati degli interventi effettuati (ad esempio, prescrivendo ai lavoratori che si assentino dall'ufficio per ferie l'attivazione di modalità che consentano di inviare automaticamente messaggi di posta elettronica ad un altro recapito accessibile: si vedano le Linee guida in materia di lavoro per posta elettronica e Internet approvate dal Garante e pubblicate nella G.U. n. 58 del 10 marzo 2007).

L'accesso ai sistemi informatici deve essere protetto da un qualunque sistema di autenticazione, costituito da UserName e Password (ved. regole 1 e 2 dell'Allegato B).
La UserName è attribuita dal Titolare in modo univoco: ad ogni Incaricato deve corrispondere una UserName diversa da quella degli altri Incaricati abilitati (ved. regola 6 dell'Allegato B).
La UserName deve essere disattivata quando l'Incaricato è rimosso e la stessa può essere attribuita ad un nuovo Incaricato (ved. regole 6 e 8 dell'Allegato B).
La Password è personale e segreta (ved. regole 3 e 4 dell'Allegato B).
Tuttavia, in caso di assenza dal lavoro per qualunque motivo (servizio, permesso, ferie, malattia, maternità, ecc.) e per inderogabili esigenze operative, essa può essere comunicata al Titolare o all'Incaricato all'Amministrazione del sistema. L'Incaricato, al suo rientro dovrà immediatamente effettuare il Cambio Password (ved. regola 10 dell'Allegato B).
Per limitare questa pratica, almeno per quanto riguarda la posta elettronica, l'Incaricato deve, in caso di ferie, attivare la procedura di invio della stessa ad un altro indirizzo prestabilito.
La regola 5 dell'Allegato B, relativa a composizione, lunghezza minima e sostituzione della Password, e la regola 7 dell'Allegato B, relativa alla disattivazione delle Password per inutilizzo, non devono essere applicate.

2.3. *Sistema di autorizzazione (modalità applicative delle regole di cui ai punti 12, 13 e 14 dell'Allegato B)*

Qualora sia necessario diversificare l'ambito del trattamento consentito, possono essere assegnati agli incaricati singolarmente o per categorie omogenee corrispondenti profili di autorizzazione, tramite un sistema di autorizzazione o funzioni di autorizzazione incorporate nelle applicazioni software o nei sistemi operativi, così da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento.

L'accesso riservato a funzioni specifiche (es. Internet) od a particolari base dati (es. Banche) può essere effettuato tramite qualunque sistema di autorizzazione, anche una Password specifica.

2.4. *Altre misure di sicurezza (modalità applicative delle regole di cui ai punti 15, 16, 17, 18 dell'Allegato B)*

I soggetti di cui al paragrafo 1 assicurano che l'ambito di trattamento assegnato ai singoli incaricati, nonché agli addetti alla gestione o alla manutenzione degli strumenti elettronici, sia coerente con i princìpi di adeguatezza, proporzionalità e necessità, anche

attraverso verifiche periodiche, provvedendo, quando è necessario, ad aggiornare i profili di autorizzazione eventualmente accordati.

Il Titolare deve verificare periodicamente che i trattamenti siano effettuati correttamente e che gli scopi di eventuali accessi riservati non siano disattesi (ved. regola 15 dell'Allegato B).

Gli aggiornamenti periodici dei programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici (ad esempio, antivirus), anche con riferimento ai programmi di cui all'art. 615-quinquies del codice penale, nonché a correggerne difetti, sono effettuati almeno annualmente. Se il computer non è connesso a reti di comunicazione elettronica accessibili al pubblico (linee Adsl, accesso a Internet tramite rete aziendale, posta elettronica), l'aggiornamento deve essere almeno biennale.

I dati personali devono essere protetti contro il rischio di intrusione o di accessi non consentiti da appositi dispositivi software (antivirus, firewall, spyware, ecc.) e da aggiornamenti del software di sistema e applicativo almeno annuale o, se il computer non è connesso a Internet, biennale (ved. regole 16 e 17 dell'Allegato B).
Vi consigliamo vivamente di aggiornarli automaticamente, altrimenti:

- nel caso dei dispositivi software, non potrete più utilizzare i computer perché saranno infettati da ogni sorta di virus che renderanno inaffidabili e, spesso, illeggibili i vostri dati;
- nel caso di aggiornamenti del software di sistema e applicativo, essi spesso contengono correzioni di errori del software originale o modifiche essenziali per la tutela dei vostri dati.

I dati possono essere salvaguardati anche attraverso il loro salvataggio con frequenza almeno mensile. Il salvataggio periodico può non riguardare i dati non modificati dal momento dell'ultimo salvataggio effettuato (dati statici), purché ne esista una copia di sicurezza da cui effettuare eventualmente il ripristino.

I dati personali devono essere protetti contro il rischio di perdita accidentale da salvataggi, anche delle sole modifiche, almeno mensili (ved. regola 18 dell'Allegato B). Periodicamente (annualmente) occorre effettuare un salvataggio totale che servirà come copia di sicurezza per il ripristino in caso di anomalie.

2.5. *Documento programmatico sulla sicurezza (modalità applicative delle regole di cui ai punti da 19.1 a 19.8 dell'Allegato B)*

2.5.1. *Fermo restando che per alcuni casi è già previsto per disposizione di legge che si possa redigere un'autocertificazione in luogo del documento programmatico sulla sicurezza (vedi il precedente par. 1, lett. a); art. 29 d.l. n. 112/2008 cit.), i soggetti pubblici e privati che trattano dati personali unicamente per correnti finalità amministrative e contabili, in particolare presso liberi professionisti, artigiani e piccole e medie imprese, possono redigere un documento programmatico sulla sicurezza semplificato sulla base delle indicazioni di seguito riportate.*

I soggetti che appartengono alla categoria **C** possono sostituire il **Documento Semplificato Sulla Sicurezza (DSSS)** con una **Dichiarazione sostitutiva dell'atto di notorietà**.

Il documento deve essere redatto prima dell'inizio del trattamento e deve essere aggiornato entro il 31 marzo di ogni anno nel caso in cui, nel corso dell'anno solare precedente, siano intervenute modifiche rispetto a quanto dichiarato nel precedente documento.

Il documento deve essere redatto prima dell'inizio del trattamento e scade al 31 marzo di ogni anno.
Entro tale data, se nel corso dell'anno precedente sono intervenute modifiche relative alla sicurezza dei dati, il documento deve essere aggiornato, altrimenti potrete compilare una **Dichiarazione di estensione di validità** dello stesso.

Il documento deve avere i seguenti contenuti:

a) le coordinate identificative del titolare del trattamento, nonché, se designati, gli eventuali responsabili. Nel caso in cui l'organizzazione preveda una frequente

modifica dei responsabili designati, potranno essere indicate le modalità attraverso le quali è possibile individuare l'elenco aggiornato dei responsabili del trattamento;

Il documento deve indicare i dati identificativi del Titolare e del Responsabile o dei Responsabili.

b) *una descrizione generale del trattamento o dei trattamenti realizzati, che permetta di valutare l'adeguatezza delle misure adottate per garantire la sicurezza del trattamento. In tale descrizione vanno precisate le finalità del trattamento, le categorie di persone interessate e dei dati o delle categorie di dati relativi alle medesime, nonché i destinatari o le categorie di destinatari a cui i dati possono essere comunicati;*

Il documento deve contenere una descrizione generale dei trattamenti, comprendente le finalità e le modalità degli stessi (es. gestione con base dati e archivi cartacei), quali tipologie di dati contengono (personali, sensibili o giudiziari) ed a quali categorie sono comunicati (es. incaricati, commercialista, Pubblica Amministrazione, ecc.).

c) *l'elenco, anche per categorie, degli incaricati del trattamento e delle relative responsabilità. Nel caso in cui l'organizzazione preveda una frequente modifica dei responsabili designati, potranno essere indicate le modalità attraverso le quali è possibile individuare l'elenco aggiornato dei responsabili del trattamento con le relative responsabilità;*

Il documento deve contenere l'elenco dei Responsabili, se previsti, e degli Incaricati abilitati. Se si prevede una frequente modifica dell'elenco, si può indicare il luogo ove esiste sempre un elenco aggiornato.

d) *una descrizione delle altre misure di sicurezza adottate per prevenire i rischi di distruzione o perdita, anche accidentale, dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.*

Il documento deve contenere l'elenco e la descrizione delle misure di sicurezza adottate e da adottare.

N.B. Le regole dalla 20 alla 26 dell'Allegato B al Codice Privacy devono sempre essere applicate.

3. Modalità applicative per i trattamenti realizzati senza l'ausilio di strumenti elettronici (modalità applicative delle regole di cui ai punti 27, 28 e 29 dell'Allegato B)

I soggetti di cui al paragrafo 1 possono adempiere all'obbligo di adottare le misure minime di sicurezza di cui all'art. 35 del Codice applicando le misure contenute nell'Allegato B) relativamente ai trattamenti realizzati senza l'ausilio di strumenti elettronici (regole da 27 a 29 dello stesso Allegato B)), con le modalità semplificate di seguito individuate.

L'utilizzo delle misure di sicurezza semplificate è autorizzato solo per le aziende delle categorie **B** e **C**.

3.1. *Agli incaricati sono impartite, anche oralmente, istruzioni finalizzate al controllo e alla custodia, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti e dei documenti contenenti dati personali.*

Tutti gli Incaricati devono ricevere istruzioni, anche orali, circa i trattamenti consentiti e la custodia dei dati loro affidati.

3.2. *Quando gli atti e i documenti contenenti dati personali sensibili o giudiziari sono affidati agli incaricati del trattamento per lo svolgimento dei relativi compiti, i medesimi atti e documenti sono controllati e custoditi dai medesimi incaricati fino alla restituzione in*

modo che a essi non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate.

I documenti cartacei devono essere "guardati a vista" dall'Incaricato ed archiviati in un contenitore protetto al termine della loro consultazione.

C Aziende che trattano dati personali non sensibili o dati sensibili dei loro dipendenti o collaboratori, relativi allo stato di salute, senza indicazione della diagnosi, o all'adesione a sindacati

Queste aziende sono tenute alla totale osservanza di quanto disposto dall'**Allegato B** al Codice Privacy con i criteri applicativi esposti nel Provvedimento del Garante del 27 novembre 2008, come quelle della categoria **B**, ma possono sostituire la redazione del Documento Semplificato Sulla Sicurezza (ved. punto 2.5 del Provvedimento e regola 19 dell'Allegato B) con una Dichiarazione sostitutiva dell'atto di notorietà, nella quale dichiarano di aver adottato almeno tutte le misure minime di sicurezza previste dall'Allegato B con l'interpretazione fornita dal sopraccitato Provvedimento.

Vi invitiamo a prestare molta attenzione a quanto sottoscrivete: si tratta di un'autocertificazione che, se falsa, vi può portare in sede penale.

Vi ricordo, per esempio, che l'utilizzo di un impianto di videosorveglianza con registrazione e l'archiviazione di curricula contenenti dati sensibili sono "trattamenti di dati sensibili".
Se trattate dati sensibili, eccetto quelli relativi allo stato di salute e all'adesione a sindacati dei vostri dipendenti, non potete sottoscriverla.
Se non siete sicuri di aver adottato almeno tutte le misure di sicurezza previste, non dovete sottoscriverla.
Altrimenti vi toccano, per il reato di "falsità nelle dichiarazioni rese al Garante", fino a tre anni di reclusione e fino a due anni per ogni misura minima non adottata.
Siamo sempre restii a parlare di galera, ma questa volta è proprio necessario!!!

L'alternativa, che non vi esonera dall'adottare le misure minime di sicurezza previste, è compilare il Documento Semplificato Sulla Sicurezza (DSSS), come riportato alle pagine 12 e 13 di questo file.

Misure minime di sicurezza per trattamenti di dati personali

Misura di sicurezza	*Trattamento di dati con strumenti elettronici*		
	Categoria A	***Categoria B***	***Categoria C***
Istruzioni al trattamento	scritte	orali	orali
Autenticazione			
abilitazione al trattamento	obbligatoria	obbligatoria	obbligatoria
UserName univoco	diverso da utenti abilitati e rimossi	diverso da utenti abilitati	diverso da utenti abilitati
password personale e segreta	obbligatoria	obbligatoria	obbligatoria
lunghezza minima password	8 chr.	---	---
cambio password (**1**)	trimestrale/ semestrale	se resa nota	se resa nota
disattivazione password	utenti rimossi o inutilizzo oltre 6 mesi	utenti rimossi	utenti rimossi
custodia password	obbligatoria	---	---
Autorizzazione			
accesso a base dati, cartelle e files	controllata dall'S.O.	qualunque sistema	qualunque sistema
elenco autorizzazioni	annuale	---	---
Misure anti-intrusione			
installazione antivirus e firewall	obbligatorio	obbligatorio	obbligatorio
aggiornamento antivirus e firewall (**2**)	trimestrale	annuale	annuale
aggiornamento sistema operativo (**3**)	semestrale	annuale	annuale
Salvataggio dei dati			
frequenza minima (**4**)	settimanale	mensile	mensile
copie di sicurezza	custodite e protette	obbligatorie	obbligatorie
distruzione supporti non utilizzati	obbligatoria	obbligatoria	obbligatoria
ripristino dei dati	entro 7 giorni	entro 7 giorni	entro 7 giorni
Documento sulla sicurezza dei dati	DPSS	DSSS (5)	Autocertificazione
scadenza	entro il 31 marzo	entro il 31 marzo	entro il 31 marzo
elenco trattamenti	obbligatorio	obbligatorio	---
distribuzione dei compiti	obbligatorio	obbligatorio	---
analisi dei rischi	obbligatorio	---	---
misure adottate e da adottare	obbligatorio	obbligatorio	---
descrizione disaster recovery	obbligatorio	facoltativo	---
previsione interventi formativi	obbligatorio	facoltativo	---
descrizione trattamenti esterni	obbligatorio	facoltativo	---
cifratura o separazione dei dati	solo per dati relativi a salute e vita sessuale	---	---
relazione accompagn. al bilancio d'esercizio	annuale, se dovuta	annuale, se dovuta	annuale, se dovuta
Installazione e Manutenzione			
certificato di conformità	obbligatorio	obbligatorio	obbligatorio
	Trattamento di dati senza strumenti elettronici		
Istruzioni al trattamento	scritte	orali	orali
Modalità di trattamento			
controllo a vista della documentazione	obbligatorio	obbligatorio	obbligatorio
registro degli accessi alla documentazione	obbligatorio	---	---

(1) Per i soggetti della categoria **A**, nel trattamento di dati non sensibili, il cambio password è almeno semestrale
Per i soggetti delle categorie **B** e **C** il cambio password è richiesto solo se la Password è portata a conoscenza di terzi

(2) Per i soggetti della categoria **A**, nel trattamento di dati non sensibili, l'aggiornamento dell'antivirus è almeno semestrale

(3) Per i soggetti della categoria **A**, nel trattamento di dati non sensibili, l'aggiornamento del sistema operativo è almeno annuale

(4) Per i soggetti delle categorie **B** e **C** il salvataggio dei dati può essere limitato ai soli aggiornamenti

(5) Se non esistono variazioni, il DSSS può essere sostituito da una Dichiarazione di estensione di validità